

**PCT**WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau

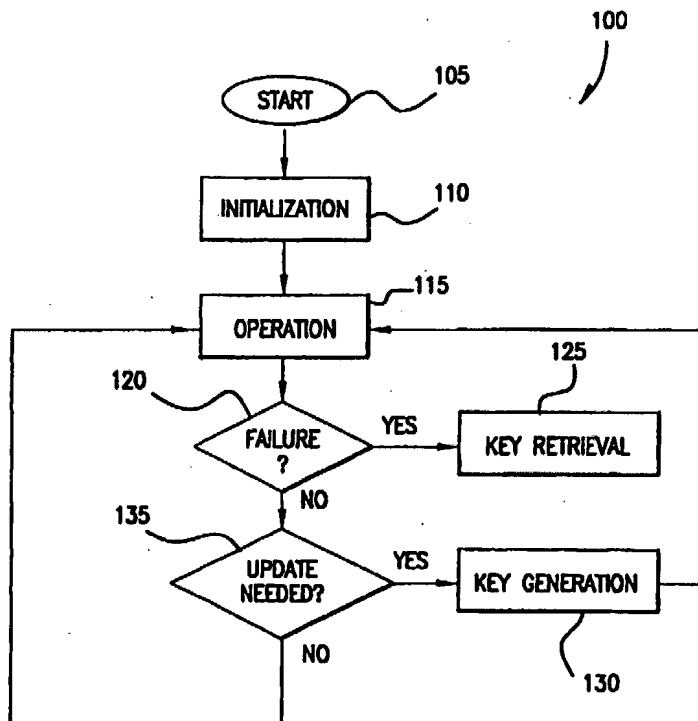
## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>6</sup> : <b>H04K 1/00</b>		<b>A1</b>	(11) International Publication Number: <b>WO 00/19652</b>
			(43) International Publication Date: <b>6 April 2000 (06.04.00)</b>
(21) International Application Number: <b>PCT/US99/22710</b>		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: <b>1 October 1999 (01.10.99)</b>			
(30) Priority Data: 60/102,633 1 October 1998 (01.10.98) US 60/131,833 29 April 1999 (29.04.99) US			
(71)(72) Applicants and Inventors: POOVENDRAN, Raadhakrishnan [LK/US]; P.O. Box 474, Greenbelt, MD 20768 (US). CORSON, Mathew, Scott [US/US]; 10122 Ashwood Drive, Kensington, MD 20895 (US). BARAS, John, S. [US/US]; 10912 Burbank Drive, Potomac, MD 20854 (US).			
(74) Agents: SOKOHL, Robert, E. et al.; Sterne, Kessler, Goldstein & Fox P.L.L.C., Suite 600, 1100 New York Avenue, N.W., Washington, DC 20005-3934 (US).		<p><b>Published</b></p> <p><i>With international search report.</i></p> <p><i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>	

(54) Title: DISTRIBUTED SHARED KEY GENERATION AND MANAGEMENT USING FRACTIONAL KEYS

## (57) Abstract

A class of distributed key generation (130) and recovery (125) approaches is presented, suitable for group communication systems where the group membership must be tightly controlled. The proposed key generation (130) approach allows entities which may have only partial trust in each other to jointly generate (130) a shared key without the aid of an external third party. The group collectively generates (130) and maintains a dynamic group binding parameter (110), and the shared key is generated (110) using a pseudorandom function (110) using this parameter as a seed. The methods employ distributed algorithms based on fractional keys (FK) (515). The proposed methods allow the members to automatically update the keys in a periodic manner without any assistance from an external third party, and to do so using verifiable secret sharing techniques. The key retrieval method (125) does not require the keys to be stored in an external retrieval center. Note that many Internet-based applications may have these requirements.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

WO 00/19652

PCT/US99/22710

## **Distributed Shared Key Generation and Management Using Fractional Keys**

5

10

### ***Field of the Invention***

The invention described herein pertains to communications, and more particularly to information security.

15

### ***Related Art***

20

Cryptographic key generation and management is an important problem in multicast and group communications (R. Canetti and Pinkas, B., "A taxonomy of multicast security issues," in *Internet-Draft* (1998); Harney, H. and Muckenhirn, C., "GKMP Architecture," *RFC 2093* (1997); Harney, H. and Muckenhirn, C., "GKMP Architecture," *RFC 2094* (1997); Ballardie, A., "Scalable Multicast Key Distribution," *RFC 1949* (1996); Poovendran, R., *et al.*, "A Scalable Extension of Group Key Management Protocol," *Proc. 2nd Ann.*

WO 00/19652

PCT/US99/22710

-2-

5     *ATIRP Conf.*, Maryland, pp. 187-191 (1998), incorporated herein by reference). In many instances, it is desirable to generate a group *shared key* (SK) for efficient intra-group communications. However, having the same SK implies that all the group membership is at the same trust level. In a distributed, multicast group, it is often not possible nor desirable to have the *same* trust level throughout the group. One may be tempted to suggest that a single trust level can be defined by choosing the lowest possible trust level as the group trust level. Though such a straightforward approach is feasible, one can do better by compartmentalizing the group based on local trust levels (*Id.*). Such a compartmentalization inevitably  
10     least to *clustering* of a given group. Compartmentalization also helps in having a better control over the set of key management and distribution functions as noted in (*Id.*).

15     While the entities in each cluster may share a common trust level, it may be that the clusters are mutually suspicious and have only *partial* trust in each other. Thus, a mechanism is desired that permits mutually suspicious parties to come together to generate a shared key. In order to avoid involving (and potentially paying) a third party, it is also desirable that the scheme involve only the group members and not external parties.

20     Some schemes (such as Harney, H. and Muckenhirn, C., "GKMP Architecture," *RFC 2093* (1997); Harney, H. and Muckenhirn, C., "GKMP Architecture," *RFC 2094* (1997); Ballardie, A., "Scalable Multicast Key Distribution," *RFC 1949* (1996)) propose to replace the traditional (external) Key Distribution Center (KDC) with a *Group Controller* (GC) which can generate and distribute the keys. However, in these approaches, a single member is allowed to  
25     generate the keys. This means that group members must place complete trust in this group member. In (Poovendran, R., *et al.*, "A Scalable Extension of Group Key Management Protocol," *Proc. 2nd Ann. ATIRP Conf.*, Maryland, pp. 187-191 (1998)), a *panel* of members are allowed to generate the keys. However, this reference does not present any explicit distributed key generation scheme.

WO 00/19652

PCT/US99/22710

-3-

(Note: The following references are incorporated herein by reference:  
Bellare and Micali, "Non-Interactive Oblivious Transfer and Applications," in  
*Advances in Cryptology -- Crypto '89*, Springer-Verlag (1989), pp. 547-557;  
Poovendran *et al.*, "A Distributed Shared Key Generation Procedure Using  
5 Fractional Keys," *Proceedings of the MILCOM '98*, Boston, MA (Oct. 1998);  
Simmons, G.J., "An Introduction to Shared Secret and/or Shared Control  
Schemes and Their Applications," in *Contemporary Cryptology: The Science of  
Information Integrity*, Simmons, G.J., ed., IEEE Press (1992), pp. 441-497.)

### *Summary of the Invention*

10           The invention described herein represents a new class of distributed key  
generation and recovery methods suitable for group communication systems  
where the group membership must be tightly controlled. The key generation  
approach allows entities which may have only partial trust in each other to jointly  
generate a shared key without the aid of an external third party. The group  
15 collectively generates and maintains a dynamic group binding parameter, and the  
shared key is generated using a pseudorandom function using this parameter as a  
seed. The methods employ distributed algorithms based on fractional keys (FK).  
The methods allow the members to automatically update the keys in a periodic  
manner without any assistance from an external third party, and to do so using  
20 verifiable secret sharing techniques. The key retrieval method does not require the  
keys to be stored in an external retrieval center. Note that many Internet-based  
applications may have these requirements.

### *Features and Advantages*

25           The invention described herein has the feature of developing a shared key  
based on components associated with respective members of a cluster. The  
invention has the additional feature of a dynamic group binding parameter that

WO 00/19652

PCT/US99/22710

-4-

serves a seed for development of the shared key. The invention has the advantage of allowing cooperative key generation without requiring action by an independent party. The invention has the further advantage of allowing key retrieval without requiring the archiving of keys at an external retrieval center.

5

### *Brief Description of the Figures*

The foregoing and other features and advantages of the invention will be apparent from the following, more particular description of a preferred embodiment of the invention, as illustrated in the accompanying drawings.

10

FIG. 1 is a flowchart illustrating the overall operation of an embodiment of the invention.

FIG. 2 is an example system implementing the invention.

FIG. 3 is a flowchart illustrating the initialization process as performed by a security manager, according to an embodiment of the invention.

15

FIG. 4 is a flowchart illustrating the initialization process as performed by cluster members in a distributed fashion, according to an embodiment of the invention.

FIG. 5 is a flowchart illustrating subsequent key generation, according to an embodiment of the invention.

20

FIG. 6 is a flowchart illustrating subsequent key generation using ElGamal public key pairs, according to an embodiment of the invention.

FIG. 7 is a flowchart illustrating key recovery, according to an embodiment of the invention.

25

FIG. 8 is a flowchart illustrating verification of security manager-based initialization, according to an embodiment of the invention.

FIG. 9 is a flowchart illustrating verification of distributed initialization, according to an embodiment of the invention.

FIG. 10 illustrates an example computing environment of the invention.

WO 00/19652

PCT/US99/22710

-5-

### ***Detailed Description of the Preferred Embodiments***

5 A preferred embodiment of the present invention is now described with reference to the figures where like reference numbers indicate identical or functionally similar elements. Also in the figures, the left most digit of each reference number corresponds to the figure in which the reference number is first used. While specific configurations and arrangements are discussed, it should be understood that this is done for illustrative purposes only. A person skilled in the relevant art will recognize that other configurations and arrangements can be used without departing from the spirit and scope of the invention. It will be apparent to a person skilled in the relevant art that this invention can also be employed in 10 a variety of other devices and applications.

#### ***I. Properties of the Key Generation and Management Method***

The following notation is used to describe the different entities involved in the method:

- 15  $\alpha_{i,j}$ : The one-time pad of the  $i$ th member at the  $j$ th key update iteration.
- $\theta_j$ : The group binding parameter at the  $j$ th key update iteration.
- $\{K_i, K_i^{-1}\}$ : Public key pair of the member  $i$ . This pair is assumed to be updated appropriately to preserve the integrity and confidentiality of any communication transaction by and with member  $i$ .
- 20  $FK_{i,j}$ : The FK of the  $i$ th member at the  $j$ th key update iteration.
- $HFK_{i,j}$ : The *hidden* FK (HFK) of the  $i$ th member at the  $j$ th key update iteration.
- $SK_j$ : The group SK at the  $j$ th key update instance.

WO 00/19652

PCT/US99/22710

-6-

$A \rightarrow B:X$ : Principal  $A$  sends principal  $B$  a message  $X$ .

In an embodiment of the invention, the message format is

$\left\{ \left\{ T_i, M, j, Msg \right\}_{K_i^{-1}} \right\}_{K_R}$ , where the variables are defined as follows:

- $T_i$ : a real-valued, wallclock time stamp generated by member  $i$
- 5     •  $M$ : denotes the *mode* of operation, with "I" for Initialization mode, "G" for Generation mode, and "R" for key Recovery mode.
- $j$ : integer-valued, denotes the current iteration number.
- $Msg$ : the message to be sent.
- $K_i^{-1}$ : denotes the private key of the sender  $S$ .
- 10    •  $K_R$ : public key of the receiver  $R$ .

The following properties are desirable for a multiparty key generation scheme:

- An FK contributed by a participating member should have the same level of security as the group SK.
- 15    • A single participating member, without valid permissions, should not be able to obtain the FK of another member.
- If a FK-generating member has physically failed, been compromised or removed, the remaining FK-generating members should be able to jointly recover the FK of the failed member.

20     The first property simply states that the distributed key generation scheme has to be such that each FK space has at least the same size as the final SK space. Hence, each member may generate FK of different size but, when combined, they lead to a fixed length SK. The second property has to do with the need for protection of individual FKs that is desired in light of the absence of a centralized

25     key generation scheme. In the current scheme, every member performs an operation to hide its FK such that, when all the hidden FKs (HFKs) and the group



WO 00/19652

PCT/US99/22710

-7-

parameter are combined, the net result is a new SK. Even if an HFK is known, the problem of obtaining the actual FK or the SK needs further computation. The requirements of the FK concealment mechanism are described in greater detail below.

5           If a contributing member physically fails, becomes compromised, or has to leave the multicast group, or cluster, then it becomes necessary to replace the existing member with a new member. Hence, the newly-elected member should be able to securely recover the FK generated by the replaced member. However, to ensure the integrity of the scheme, this recovery should be possible only if all  
10           the remaining contributing members cooperate. This feature deviates significantly from the existing key generating schemes (Harney, H. and Muckenhirn, C., "GKMP Architecture," *RFC 2093* (1997); Harney, H. and Muckenhirn, C., "GKMP Architecture," *RFC 2094* (1997); Ballardie, A., "Scalable Multicast Key Distribution," *RFC 1949* (1996)). The requirement that an individual member  
15           acting alone not be able to obtain the FKs of other contributing members is similar to protecting individual private keys in public key cryptography systems.

The following is a list of assumptions regarding the method:

- There exist two commutative operators  $\odot$  and  $\diamond$  which form an abelian group when operating on the set of keys.
- 20       • It is computationally difficult to perform cryptographic analysis on a cryptographically-secure random key by search methods if the key length is sufficiently large.
- The keys are all  $L$  bits in length, and all members know its length.
- The number of participants in generating the KS is fixed as  $n$   
25       (where  $n$  may be a function of  $\odot$  and  $\diamond$ ).
- There is a mechanism for certifying the members participating in the key generation procedure, for securely exchanging the quantities required in the algorithm and for authenticating the source of these quantities.
- 30       • Every member has the capability to generate a cryptographically-secure random number of length  $L$  bits or longer.

WO 00/19652

PCT/US99/22710

-8-

With the assumptions above, the key management scheme can be described in terms of three major processes:

1. Initialization, which includes secure initial one-time pad and binding parameter generation and distribution;
- 5        2. Key Generation, an iterative process including fractional, hidden and shared-key generation; and
3. Key Retrieval, a process that is required only in the case of a member node failure or compromise.

These processes are collectively illustrated in process 100 of FIG. 1. Process 100 begins with a step 105. In a step 110, the key management process is initialized. Here, initial one-time pads are generated for each member. In addition, a binding parameter is generated and distributed to each member, permitting each member to generate the same key, a shared key SK. In a step 115, the members can operate securely using the SK. If, in a step 120, a failure occurs at a member's node, such as a compromise of the member or an equipment failure, then key retrieval is performed in a step 125. Here, recovery of the parameters associated with the failed node is performed. In a step 130, a new binding parameter is generated and new one-time pads are created. Operations then resume at step 115.

20        If, in step 120, no failure occurs, process 100 continues with a step 135. Here, a determination is made as to whether an update of the SK is needed. This may be required, for example, if a member leaves the cluster. Alternatively, an operation may simply require periodic updating of the SK. If an update is needed, key generation step 130 is performed. Operations then resume at step 115.

25        The processes of initialization, key generation, and key retrieval are described in greater detail below.

## ***II. Initialization***

WO 00/19652

PCT/US99/22710

-9-

A Group Initiator (GI) first selects a set of  $n$  FK-generating members of a cluster, and the GI may be one of these members. The GI can then contact a Security Manager (SM)—a third party who is *not* a FK-generating member—who generates the initial pads and the binding parameter and distributes them to the members. This is illustrated by system 200 of FIG. 2. Member 1, group initiator 210, is shown contacting security manager 250, who then distributes the necessary data to member 1 through 4, labelled 210 through 240, respectively. The data flow for this embodiment is illustrated by dotted lines. In an alternative embodiment, GI 210 initiates a distributed procedure among the group members (illustrated by solid lines) to create these quantities without the aid of an external party.

#### A. SM-Based Initialization

The process of initialization by an SM is illustrated in FIG. 3, process 300, according to an embodiment of the invention. Process 300 begins with a step 305. In a step 310, the GI generates an initial random one-time pad,  $\alpha_{i,1}$ , for each member  $i$ . In a step 315, an initial binding parameter  $\theta_1$  is computed such that  $\alpha_{1,1} \oplus \alpha_{2,1} \oplus \dots \oplus \alpha_{n,1} = \theta_1$ . In steps 320 through 340,  $\alpha_{i,1}$  and  $\theta_1$  are sent to each member  $i$ . In step 320, index  $i$  is initialized. In steps 325 and 330, the initial pads and binding parameter are distributed to member  $i$ , as

$$SM \rightarrow i: \left\{ \left\{ T_{SM}, 1, 1, \alpha_{i,1}, \theta_1 \right\}_{K_{SM}^{-1}} \right\}_{K_i}$$

In step 335, index  $i$  is incremented. In step 340, a determination is made as to whether  $\alpha_{i,1}$  and  $\theta_1$  have been sent to all members  $i$ . If not, then  $\alpha_{i,1}$  and  $\theta_1$  are sent to the next member  $i$ . The process concludes with a step 345. At the conclusion of process 300, each member has  $\theta_1$ , on which a common SK can be based.

#### B. Distributed Initialization

WO 00/19652

PCT/US99/22710

-10-

In an alternative embodiment, initialization can be performed through a cooperative process involving all members, illustrated as process 400 of FIG. 4. The GI (assumed to be a member and denoted in process 400 by the index 1) can perform the following steps (see also Koblitz, N., *Cryptologia* 317-326 (1997), incorporated herein by reference) to generate the initial parameters of the group. Process 400 begins with a step 405. In a step 410, member 1 generates two uniformly-distributed random quantities  $\gamma$  and  $v_{1,1}$  of bit length  $L$ . In a step 415, member 1 operates on these two quantities as  $\gamma \oplus v_{1,1} = \delta_1$ . In a step 420, member 1 sends the result to member 2 (the "next" member in the group) as  $1 \rightarrow 2$ :

$$10 \quad \left\{ \left\{ T_1, I, 1, \delta_1 \right\}_{K_1^{-1}} \right\}_{K_2}$$

Starting with member 2, each member  $i$  calculates its own  $\delta_i$  based on the previous member's  $\delta_{i-1}$ , and sends  $\delta_i$  to the next member. This is illustrated in steps 425 through 450. In step 425, the index  $i$  is initialized to 2. In step 430, member  $i$  generates a uniform random variable  $v_{i,1}$  of bit length  $L$ . In step 435, member  $i$  then operates on the quantity it received from member  $i-1$  as  $\delta_{i-1} \oplus v_{i,1} = \delta_i$ . In step 440, member  $i$  then sends the result to member  $i+1$  as  $i \rightarrow i+1$ :

$$15 \quad +1: \left\{ \left\{ T_i, I, 1, \delta_i \right\}_{K_i^{-1}} \right\}_{K_{i+1}}$$

In step 445,  $i$  is incremented. If, as determined in step 450, each of the  $n$  members has not generated a respective value  $\delta_i$ , the process returns to step 430, where the next member  $i$  generates its uniform random variable  $v_{i,1}$ .

Eventually, the group member  $i = n$  receives  $\delta_{n-1}$  and, in a step 455, generates a uniformly-distributed random quantity  $v_{n,1}$  of bit length  $L$ . In a step 460, member  $n$  performs  $\delta_{n-1} \oplus v_{n,1} = \delta_n$ . In a step 470, member  $n$  securely sends  $\delta_n$  to the initiating member  $i = 1$  as  $n \rightarrow 1$ :  $\left\{ \left\{ T_n, I, 1, \delta_n \right\}_{K_n^{-1}} \right\}_{K_1}$ . In a step 475,

20

WO 00/19652

PCT/US99/22710

-11-

the GI (member 1) then recovers  $\delta_n$  and performs  $\gamma \oplus \delta_n = \theta_1$ . In steps 480 through 494, member 1 sends  $\theta_1$  to each member  $i$ . In step 480, the index  $i$  is initialized to 2. In step 485, member 1 sends  $\theta_1$  to member  $i$  as

$$1 \rightarrow i: \left\{ \left\{ T_1, I, 1, \theta_1 \right\}_{K_i^{-1}} \right\}_{K_i}$$

5            In step 490, each member  $i$  privately computes  $\alpha_{i,1} = \theta_1 \oplus v_{i,1}$ . In step 492, the index  $i$  is incremented. If, in step 494,  $i > n$ , so that each member  $i$  has received  $\theta_1$  and privately computed a respective  $\alpha_{i,1}$ , then the process 400 concludes with a step 496. Otherwise, the process returns to step 485, where member 1 sends  $\theta_1$  to another member. At the conclusion of process 400, each member has  $\theta_1$ , on which a common SK can be based.

Note that these two approaches of initialization (security manager-controlled initialization and distributed initialization) are not equivalent unless additional security assumptions are made. For example, in the case of distributed initialization within the group, the following can be done.

15            Assume that members  $i-1$  and  $i+1$  conspire to obtain the secret member  $i$ , where the numerical ordering corresponds to the order of message passing in the distributed algorithm.

1. Member  $i-1$  sends  $\delta_{i-1}$  to member  $i$  as per the algorithm, and *also* to member  $i+1$  without  $i$ 's knowledge.
- 20            2. Member  $i$ , who is unaware of the conspiracy between  $i-1$  and  $i+1$ , computes  $\delta_i = \delta_{i-1} \oplus v_{i,1}$  and sends it to member  $i+1$  securely.
3. Member  $i+1$  can now compute  $v_{i,1} = \delta_{i-1} \oplus \delta_i$  and obtain the secret  $v_{i,1}$  of member  $i$ .

25            However, the secret  $v_{i,1}$  generated by member  $i$  become part of the pads (i.e. the  $\alpha$ 's) of members  $i-1$  and  $i+1$ . Hence, application of this initialization assumes that the parties are benign.

WO 00/19652

PCT/US99/22710

-12-

### III. Key Generation

The key generation algorithm is an iterative process depicted in FIG. 5 as process 500. Each successive key generation, iteration  $j$ , requires as input a set of one-time pads  $\alpha_{i,j}$ ,  $i = 1, \dots, n$ , and the binding parameter  $\theta_j$ , which are obtained from the initialization process (e.g., process 300 or process 400) for iteration  $j = 1$ , and from the preceding iterations for  $j > 1$ .

The iterative key generation process, according to an embodiment of the invention, consists of the following. Process 500 begins with a step 505. In steps 510 through 535, each member  $i$  generates a cryptographically-secure random number, fractional key  $FK_{i,j}$ , and sends it to every other member  $m$ . In step 510, index  $i$  is initialized to 1. In step 515, member  $i$  generates random number  $Fk_{i,j}$ . In step 520, member  $i$  generates a hidden fractional key  $HFK_{i,j} = \alpha_{i,j} \otimes FK_{i,j}$ . In step 525, member  $i$  sends  $HFK_{i,j}$  to every other member  $m$  as

$$i \rightarrow m: \left\{ \left\{ T_i, G, j, HFK_{i,j} \right\}_{K_i^{-1}} \right\}_{K_m}$$

In step 530, index  $i$  is incremented. If, as determined in step 535, each member  $i$  has created a respective  $HFK_{i,j}$  and sent it to all other members, the process continues at a step 540. Otherwise, process 500 returns to step 515, where the next member  $i$  generates its respective  $FK_{i,j}$ .

Once the exchange of  $HFK_{i,j}$ 's is complete, each member computes the new group parameter  $\theta_{j+1}$  and a new shared key  $SK_j$ . This occurs in steps 540 through 560. In step 540, index  $i$  is initialized to 1. In step 545, member  $i$  calculates the new binding parameter,  $\theta_{j+1} = \lambda \theta_j \otimes HFK_{1,j} \otimes HFK_{2,j} \otimes \dots \otimes HFK_{n,j} = FK_{1,j} \otimes FK_{2,j} \otimes \dots \otimes FK_{n,j}$ . In step 550, member  $i$  calculates a new one-time pad  $\alpha_{i,j+1} = \theta_{j+1} \otimes FK_{i,j}$  and a new shared key  $SK_j = f(\theta_{j+1})$  where  $f(\cdot)$  is a strong one-way pseudo-random function. In step 555, index  $i$  is incremented. If, in step 560,  $i > n$ , so that each member  $i$  has created a new  $\theta_{j+1}$  and a new  $SK_j$ , then the

WO 00/19652

PCT/US99/22710

-13-

process concludes with a step 565. Otherwise, process 500 returns to step 545, where the next member  $i$  calculates the new binding parameter,  $\theta_{j+1}$ .

If the resulting group parameter  $\theta_{j+1}$  is cryptographically insecure for a particular application, all members can repeat process 500 creating a new high quality group parameter  $\theta_{j+1}$ .

At the end of process 500, we have the SK for the current iteration. Note that the quantity  $\alpha_{i,j+1}$  is computed such that, for an outsider, obtaining  $\alpha_{i,j+1}$  is very hard, even if the actual shared key  $SK_j$  is compromised at any key update time interval  $(j, j+1)$ . Knowing the shared key  $SK_j$  does not reveal the group parameter  $\theta_j$  and, hence, the tight binding of the members will not be broken by the loss of the shared key.

Note the following additional features of the key scheme:

- Although all the members have each  $HFK_{i,j}$ , obtaining the  $FK_{i,j}$  or  $\alpha_{i,j+1}$  of another member involves search in the  $L$ -dimensional space, and obtaining their correct combination involves search in the  $(n-1)L$ -dimensional space. Hence, even if a fellow member becomes an attacker, that rogue member faces nearly the same computational burden in obtaining the set of  $n$  FKs as an outside cryptographic analyst; i.e. trust is *not* unconditional.
- For such an outside attacker, breaking the system requires either search in an  $L$ -dimensional space to get  $\theta$ , or  $nL$ -dimensional searches to break individual secrets of all the members. Access to all  $n$  HFKs is alone is insufficient to permit an attacker to determine the SK; for that, the attacker must also possess the current binding parameter  $\theta$  which is time-varying and never transmitted. If an SK is known to be compromised (perhaps due to traffic analysis), information regarding  $\theta$  is not obtained, since  $f(\cdot)$  is a pseudo-random function.

In an embodiment of the invention, an  $FK_{i,j}$  is used whereby  $(FK_{i,j}^{-1}, FK_{i,j})$  is an individual ElGamal public key pair for the member  $i$  at update  $j$ . The iterative key generation process for this embodiment is illustrated as process 600 of FIG. 6. Process 600 begins with a step 605. In steps 610 through

WO 00/19652

PCT/US99/22710

-14-

640, each member  $i$  develops values  $FK_{i,j}$  and  $HFK_{i,j}$  and exchanges them with other members. In step 610, index  $i$  is initialized to 1. In step 615, member  $i$  randomly picks a number  $FK_{i,j}^{-1}$  with  $0 \leq FK_{i,j}^{-1} \leq p-2$ . In step 620, member  $i$  generates  $FK_{i,j} = \alpha^{FK_{i,j}^{-1}}$ . Here,  $(FK_{i,j}^{-1}, FK_{i,j})$  is an individual ElGamal public key pair for the member  $i$  at update  $j$ . In step 625, member  $i$  generates a quantity  $HFK_{i,j} = (\alpha_{i,j} + FK_{i,j}) \bmod p$ . In step 630, member  $i$  sends  $FK_{i,j}$  and  $HFK_{i,j}$  to each other member  $m$ , in the form

$$i \rightarrow m: \left\{ \left\{ T_i, G, j, HFK_{i,j}, FK_{i,j} \right\}_{FK_{i,j}^{-1}} \right\}_{FK_{m,j}^{-1}}. \text{ In step 635, index } i \text{ is}$$

incremented. If, as determined in step 640,  $i > n$ , so that each member  $i$  has created a respective  $HFK_{i,j}$  and sent it, along with  $FK_{i,j}$ , to all other members, the process continues at a step 645. Otherwise, process 600 returns to step 615, where the next member  $i$  selects its respective  $FK_{i,j}^{-1}$ .

In steps 645 through 665, each member generates a new binding parameter  $\theta_{j+1}$  and one-time pad  $\alpha_{i,j+1}$ . In step 640, index  $i$  is initialized to 1. In step 650, each member  $i$  computes  $\theta_{j+1} = ((p - n - 3)\theta_j + \sum_{i=1}^n HFK_{i,j}) \bmod (p-1)$ , defining  $GK_{j+1}^{-1} = \theta_{j+1}$ . Each member  $i$  also computes

$$GK_{j+1} = \alpha^{GK_{j+1}^{-1}} = \prod_{i=1}^{i=n} FK_{i,j} = \prod_{i=1}^{i=n} \alpha^{FK_{i,j}^{-1}} \text{ in step 650. In step 655, member}$$

$i$  calculates  $\alpha_{i,j+1} = (GK_{j+1}^{-1} + FK_{i,j}^{-1}) \bmod p$ . In step 660, index  $i$  is

incremented. In step 665, a determination is made as to whether  $i > n$ , i.e., whether each member  $i$  has calculated the new  $\theta_{j+1}$  and a new  $\alpha_{i,j+1}$ . If so, process 600 concludes with a step 670. Otherwise, process 600 returns to step 650 so that the next member  $i$  can create a new  $\theta_{j+1}$ .



WO 00/19652

PCT/US99/22710

-15-

Note that if the resulting group key pair  $(GK_{j+1}, GK_{j+1}^{-1})$  is cryptographically insecure for a particular application, all members can repeat process 600, creating a new high quality key pair.

#### IV. Retrieval of the Fractional Key and One-time Pad of a Failed Node

5 The following steps, illustrated as process 700 of FIG. 7, are involved in recovery of the  $FK_{i,j}$  and  $\alpha_{i,j}$  of the node failed  $i$ , where  $j$  represents the iteration number in which the node was compromised or failed. The process begins with a step 705. In a step 710, any one FK-generating member—called the Recovery Initiator (RI)—initiates recovery and gives the HFK of the failed node  $i$  to the

10 newly-elected node  $i$  as  $RI \rightarrow i: \left\{ \left\{ T_{RI}, R, j, HFK_{i,j} \right\}_{K_{RI}^{-1}} \right\}_K$ . In a step 615, the RI gives the newly-elected node  $i$  the current  $SK_j$  as  $RI \rightarrow i: \left\{ \left\{ T_{RI}, R, j, SK_j \right\}_{K_{RI}^{-1}} \right\}_K$ . In a

15 step 720, distributed initialization is performed, with the following replacements: (a)  $\theta$  by  $\xi$  and (b)  $\alpha_{i,j}$  by  $\beta_{i,j}$ . Except for the changes in the notation and the number of members participating, the process for pad generation is same as for distributed initialization. Hence, at the end of this distributed pad generation, each member  $l$  has  $\beta_{l,j}$  as its pad for key recovery process, and all these pads are bound with the parameter  $\xi$ . In steps 725 through 745, each member  $l$  calculates a modified hidden fractional key  $H\hat{F}K_{l,j}$  and distributes it to newly elected

20 member  $i$ . In step 725, index  $l$  is initialized to 1. In step 730, member  $l$  computes modified hidden fractional key  $H\hat{F}K_{l,j} = \beta_{l,j} \diamond FK_{i,j}$  and sends it to the newly-elected member  $i$  as  $l \rightarrow i: \left\{ \left\{ T_l, R, j, H\hat{F}K_{l,j} \right\}_{K_l^{-1}} \right\}_K$  in step 735. In step 740, index  $l$  is incremented. In step 745, a determination is made as to whether  $l > n$ , i.e.,

WO 00/19652

PCT/US99/22710

-16-

whether each member  $l$  has calculated a modified hidden fractional key  $H\hat{F}K_{l,j}$  and distributed it to newly elected member  $i$ . If not, process 700 returns to step 730. Otherwise, process 700 continues with a step 750.

In step 750, member  $i$  combines all of the modified HFKs and recovers the fractional key  $FK_{i,j}$  using the operation  $FK_{i,j} = \lambda\xi \circledast H\hat{F}K_{i,j} \circledast \dots \circledast H\hat{F}K_{i,j} \circledast \theta_{j+1}$ . In step 755, member  $i$  extracts the one-time pad  $\alpha_{i,j}$  using the operation  $\alpha_{i,j} = HFK_{i,j} \circledast FK_{i,j}$ . The process 700 concludes with a step 760.

Note that the recovered values of  $FK_{i,j}$  and  $\alpha_{i,j}$  are unique. Once the new node recovers the fractional key of the compromised node, it can inform the other contributing members to update the iteration number  $j$  to  $j + 1$ , and then all members can execute the key generation algorithm. Note that even though the newly-elected member recovers the compromised fractional key and pad, the next key generation operation of the new node does not use the compromised key or pad. Hence, even if the attacker possesses the fractional key or pad at iteration  $j$ , it does not allow the attacker to obtain the future fractional keys or pads without any computation.

#### V. A Specific Choice of the Functions $\circledast$ and $\diamond$

A class of multiparty key generation algorithms is described above where a given instance of the class is determined by choice of function  $\circledast$ . Note that one possible choice for  $\circledast$  is the modulo addition operation with respect to a large odd prime  $p$ , denoted here with  $\oplus$ . In this case, we can deduce the following computation from the key generation algorithm:

WO 00/19652

PCT/US99/22710

-17-

$$HFK_{1,j} \oplus HFK_{2,j} \oplus \dots \oplus HFK_{n,j} = \\ FK_{1,j} \oplus FK_{2,j} \oplus \dots \oplus FK_{n,j} \oplus (n-1)\theta_j$$

To remove the effect of  $\theta_j$  on  $\theta_{j+1}$ , we should ensure that  $\lambda = (p+1-n)$  so that

$$\begin{aligned} \theta_{j+1} &= (p+1-n)\theta_j \oplus HFK_{1,j} \oplus HFK_{2,j} \oplus \dots \\ &\quad \dots \oplus HFK_{n,j} \\ &= FK_{1,j} \oplus FK_{2,j} \oplus \dots \oplus FK_{n,j} \end{aligned}$$

5 Regarding the choice of the number of members, clearly the choice of  $n=2$  is not appropriate for such a scheme. Although choosing  $n=3$  does not instantly expose a secret pad  $\alpha$ ; when a participating member becomes an attacker (i.e. a *rouge*), the following attack—called *fractional attack* (FA)—is feasible.

10 *Lemma:* When  $\oplus$  is an  $\oplus$  function, independent of how nontrivial the bit-length of the key is, choosing  $n=3$  permits a FA.

*Proof:* Assume that the time instant at which one member  $i$  ( $i=1$  or  $2$  or  $3$ ) become a *rouge* is  $j$ . At this time the member have values of  $\alpha_{1,j} = HFK_{2,j} \oplus HFK_{3,j}$ ,  $\alpha_{2,j} = HFK_{3,j} \oplus HFK_{1,j}$ ,  $\alpha_{3,j} = HFK_{1,j} \oplus HFK_{2,j}$ . Every member also has access to the current  $\theta_{j+1}$  and their own  $FK_{l,j}$  ( $l=1, 2, 3$ ). At this stage, obtaining the  $\alpha$  component of any other member is as computationally intensive as an outside attacker trying to obtain  $\theta_{j+1}$ . However, if a member, say  $i=1$ , is compromised and releases its secret  $\alpha_{1,j}$ , then each of the other members can use this and compute  $FK_{l,j} = \alpha_{1,j} \oplus \theta_j$ . Since  $\theta_{j+1} = FK_{1,j} \oplus FK_{2,j} \oplus FK_{3,j}$ , each member can now compute the other non-rouge member's FK as well.

20 This leads to the following corollary: When  $\oplus$  is an  $\oplus$  function, independent of how non-trivial the bit-length of the key, the minimum number of members to prevent a FA by a single *rouge* member for the multiparty key scheme is 4.

WO 00/19652

PCT/US99/22710

-18-

## VI. Verifiable Secret Sharing

Since there are multiple entities involved in key generation, it becomes important to have a mechanism to verify if the parameters exchanged actually contribute to the generated shared key. The verification steps can be followed at  
 5 (1) SM-based group initialization, (b) distributed group initialization, and (c)  $\theta$ -generation iteration.

### A. SM-based Initialization

In the case of the SM-based scheme, each member  $i$  needs to make sure that the SM uses non-trivial values of its  $\alpha_{i,1}$  and  $\theta_1$ . Since each member needs to protect its individual pad value, one method for openly checking correctness of the  
 10 pads is to generate a public value that will enable all the key generating members to check their correctness without revealing the actual value of the individual pads. Such a verification technique falls under the category of Verifiable Secret Sharing (VSS) (Feldman, P., "A Practical Scheme for Non-Interactive Verifiable Secret  
 15 Sharing," *Proc. of IEEE Fund. Comp. Sci.*, pp. 427-437 (1987); Pedersen, T. P., *Advances in Cryptology - CRYPTO, LNCS 576*:129-140 (1991)).

If one wants to check if the individual initial pads  $\alpha_{i,1}$  given by the security manager are "good", process 800 of FIG. 8 can be used. The process begins with a step 805. In a step 810, one member (possibly the SM) picks a very large prime  
 20 number  $q$ . The number picked should be larger than the possible range of the  $\theta$  value. In a step 820, prime number  $q$  is sent to all the members. In a step 825, the same member also sends a generator  $g$  of the multiplicative group  $q$ . In a step 830, each member picks a random polynomial  $f_i$  having a value 0 at the origin. In a step 835, each member adds the polynomial to its pad value, generates  
 25  $\hat{\alpha}_{i,1} = g^{a_{i,1} + f_i}$  and broadcasts the values to all the members. In a step 840, each

member  $i$  computes  $g^{\theta_i} = \prod_{j=1}^{J-n} \hat{\alpha}_{j,1} = g^{\theta_i}$ . In a step 845, each member

WO 00/19652

PCT/US99/22710

-19-

checks if the value is equal to  $g^{\theta_i}$  at the origin. If not, then the verification fails in a step 850. If the check of step 845 passes, then in a step 855, each member checks to see that

$$g^{a_{i,1}} = \frac{g^{\theta_i}}{\prod_{j=1}^{j=n} g^{a_{j,1}}}$$

5 If not, verification fails in step 850. Failed verification means that some or all of the members' one-time pads do not correspond to  $\theta_i$ . Process 800 concludes with a step 860.

### ***B. Distributed Initialization***

10 In the case of distributed initialization, process 900 of FIG. 9 can be used to check if the GI, member 1, has produced a  $\theta_i$  using contributions from all the group members. The process begins with a step 905. In a step 910, one member (possibly the GI) picks a very large prime number  $q$ . The number picked should be larger than the possible range of the  $\theta_i$  value. In a step 915, prime number  $q$  is sent to all the members. In a step 920, the same member also sends a generator  $g$  of the multiplicative group under  $q$  to all members. In a step 925, GI computes  $g^r$  and  $g^{v_{1,2}}$ , and makes them available to all the group members. In a step 930, each member  $i$  publishes  $g^{v_{i,1}}$  making it available only to the group members.

15 In a step 935, each member  $i$  checks if  $g^{\theta_i} = \prod_{j=1}^{j=n} g^{v_{j,1}}$ . If the equality is not true, then failed verification is indicated in a step 940. Failure (inequality) means that the binding parameter  $\theta_i$  and the individual one-time pads do not agree. Since at each step of adding their secrets members published the broadcast values, it is possible to check which member cheated if there is no collaboration. If there

20

WO 00/19652

PCT/US99/22710

-20-

is a collaboration, then the last among the collaborating member can be identified by the non-collaborating member.

Note that similar testing can be done for the key generation process.

## ***VII. Environment***

5           The present invention may be implemented using hardware, software or a combination thereof. The operations described above may be implemented in a computer system or other processing system at the node of a member. An example of such a computer system 1000 is shown in FIG. 10. The computer system 1000 includes one or more processors, such as processor 1004. The processor 1004 is connected to a communication infrastructure 1006, such as a bus or network). Various software implementations are described in terms of this exemplary computer system. After reading this description, it will become apparent to a person skilled in the relevant art how to implement the invention using other computer systems and/or computer architectures.

10           Computer system 1000 also includes a main memory 1008, preferably random access memory (RAM), and may also include a secondary memory 1010. The secondary memory 1010 may include, for example, a hard disk drive 1012 and/or a removable storage drive 1014, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, etc. The removable storage drive 1014 reads from and/or writes to a removable storage unit 1018 in a well known manner. Removable storage unit 1018, represents a floppy disk, magnetic tape, optical disk, or other storage medium which is read by and written to by removable storage drive 1014. As will be appreciated, the removable storage unit 1018 includes a computer usable storage medium having stored therein computer software and/or data.

20           In alternative implementations, secondary memory 1010 may include other means for allowing computer programs or other instructions to be loaded into computer system 1000. Such means may include, for example, a removable

WO 00/19652

PCT/US99/22710

-21-

storage unit 1022 and an interface 1020. Examples of such means may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM, or PROM) and associated socket, and other removable storage units 1022 and interfaces 1020 which allow software and data to be transferred from the removable storage unit 1022 to computer system 1000.

Computer system 1000 may also include a communications interface 1024. Communications interface 1024 allows software and data to be transferred between computer system 1000 and external devices. Examples of communications interface 1024 may include a modem, a network interface (such as an Ethernet card), a communications port, a PCMCIA slot and card, etc. Software and data transferred via communications interface 1024 are in the form of signals 1028 which may be electronic, electromagnetic, optical or other signals capable of being received by communications interface 1024. These signals 1028 are provided to communications interface 1024 via a communications path (i.e., channel) 1026. This channel 1026 carries signals 1028 and may be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an RF link and other communications channels. In an embodiment of the invention in which computer system 1000 represents the computer system of a member's node, signals 1028 comprise information flowing to and from the node, such as the encrypted form of  $\delta_i$  in step 440, and the encrypted form of  $HFK_{i,j}$  of step 525.

In this document, the terms "computer program medium" and "computer usable medium" are used to generally refer to media such as removable storage units 1018 and 1022, a hard disk installed in hard disk drive 1012, and signals 1028. These computer program products are means for providing software to computer system 1000.

Computer programs (also called computer control logic) are stored in main memory 1008 and/or secondary memory 1010. Computer programs may also be received via communications interface 1024. Such computer programs, when executed, enable the computer system 1000 to implement the present invention

WO 00/19652

PCT/US99/22710

-22-

as discussed herein. In particular, the computer programs, when executed, enable the processor 1004 to implement the present invention. Accordingly, such computer programs represent controllers of the computer system 1000. Where the invention is implemented using software, the software may be stored in a computer program product and loaded into computer system 1000 using removable storage drive 1014, hard drive 1012 or communications interface 1024. In an embodiment of the present invention, the steps of processes 300 through 900 are implemented in software that can therefore be made available to processor 1004 at a member node through any of these means.

#### 10 *VIII. Conclusion*

While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example, and not limitation. It will be apparent to persons skilled in the relevant art that various changes in detail can be made therein without departing from the spirit and scope of the invention. Thus the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.



WO 00/19652

PCT/US99/22710

-23-

***What Is Claimed Is:***

1. A method of generating and managing shared keys for a plurality of members of a cluster, comprising the steps of
  - (a) system initialization to produce a functionally generated initial shared key;
  - (b) functional generation of a next shared key; and
  - (c) key recovery in the event of either compromise or failure of a node.
2. The method of claim 1, wherein step (a) comprises the steps of:
  - (i) generating a random initial one-time pad  $\alpha_{1,2}$  for each member;
  - (ii) calculating an initial binding parameter  $\theta_1$  based on each  $\alpha_{1,2}$ , where  $\theta_1 = \alpha_{1,1} \otimes \alpha_{2,1} \otimes \dots \otimes \alpha_{n,1}$  wherein  $\otimes$  is a commutative operator; and
  - (iii) sending  $\theta_1$  and  $\alpha_{i,1}$  to each member  $i$ .
3. The method of claim 2, wherein step (iii) comprises the step of encrypting  $\theta_1$  and  $\alpha_{i,1}$  in the form

$$\left\{ \left\{ T_{SM}, I, 1, \alpha_{i,1} \right\}_{K_{SM}^{-1}} \right\}_{K_i}$$

for transmission to each member  $i$ , where

$T_{SM}$  is a timestamp generated by a security manager (SM),

$I$  is an indicator of an initialization mode,

$1$  denotes the first interaction of key generation,

$K_{sm}^{-1}$  is an encryption operation using a private component of a

private/public key pair of the security manager, and

WO 00/19652

PCT/US99/22710

-24-

$K_i$  indicates encryption using a public component of a private/public key pair of member  $i$ .

4. The method of claim 1, wherein step (a) comprises the steps of:

- (i) generation, by a member 1, of random quantities  $\gamma$  and  $v_{1,1}$ ;
- 5 (ii) calculation by the member 1, of  $\gamma \otimes v_{1,1} = \delta_1$ , wherein  $\otimes$  is a commutative operator;
- (iii) sending, by the member 1, of  $\delta_2$  to a member 2;
- (iv) receipt, by a member  $i$ , of  $\delta_{i-1}$  from a preceding member  $i-1$ ;
- (v) generation, by member  $i$ , of random quantity  $v_{i,1}$ ;
- 10 (vi) calculation, by member  $i$ , of  $\delta_{i-1} \otimes v_{i,1} = \delta_i$ ;
- (vii) sending, by member  $i$ , of  $\delta_i$  to a member  $i+1$ ;
- (viii) sending, by a last member  $n$ , of  $\delta_n$  to member 1;
- (ix) calculation, by member 1, of  $\gamma \otimes \delta_n = \theta_1$ ;
- (x) sending, by member 1, of  $\theta_1$  to each member;
- 15 (xi) calculation, by each member, of  $\theta_1 \otimes v_{i,1} = \alpha_{i,1}$ .

5. The method of claim 4, wherein step iii) comprises the step of encrypting  $\delta_1$  in the form

$$\left\{ \left\{ T_1, I, 1, \delta_1 \right\}_{K_1^{-1}} \right\}_{K_2} \text{ for transmission to member 2,}$$

step (vi) comprises the step of encrypting  $\delta_i$  in the form

20  $\left\{ \left\{ T_i, I, 1, \delta_i \right\}_{K_i^{-1}} \right\}_{K_{i+1}} \text{ for transmission to member } i+1,$

step (vii) comprises the step of encrypting  $\delta_n$  in the form

$$\left\{ \left\{ T_n, I, 1, \delta_n \right\}_{K_n^{-1}} \right\}_{K_1} \text{ for transmission to member 1, and}$$

WO 00/19652

PCT/US99/22710

-25-

step (ix) comprises the step of encrypting  $\theta_i$  in the form

$$\left\{ \left\{ T_i, I, 1, \theta_i \right\}_{K_i^{-1}} \right\}_{K_i} \text{ for transmission to member } i.$$

6. The method of claim 1, wherein step (b) comprises the steps of:

5 (i) generation, by each member  $i$ , of a cryptographically secure random number,  $Fk_{i,j}$ , where  $j$  denotes the key generation iteration;

(ii) calculation, by each member  $i$ , of  $HFK_{i,j} = \alpha_{i,j} \otimes Fk_{i,j}$ , where  $\otimes$  is a commutative operator;

(iii) sending, by each member  $i$ , of  $HFK_{i,j}$  to each other member;

10 (iv) calculation, by each member  $i$ , of  
 $\theta_{j+1} = \lambda \theta_i \otimes HFK_{i,j} \otimes HFK_{2,j} \otimes \dots \otimes HFK_{n,j}$

where  $\lambda$  is a scaling factor and  $n$  is the number of members in the cluster;

15 (v) calculation, by each member  $i$ , of  
 $\alpha_{i,j+1} = \theta_{j+1} \otimes Fk_{i,j}$

(vi) calculation, by each member  $i$ , of a shared key  
 $SK_{j+1} = f(\theta_{j+1})$

where  $f$  is a strong one way function, to form a fractionally generated next shared key.

20 7. The method of claim 6, wherein the step (iii) comprises the step of encrypting  $HFK_{i,j}$  in the form

$$\left\{ \left\{ T_i, G, j, HFK_{i,j} \right\}_{K_i^{-1}} \right\}_{K_m} \text{ for transmission to each other}$$

member  $m$ .

25 8. The method of claim 6, wherein  
 step (i) comprises the steps of:

WO 00/19652

PCT/US99/22710

-26-

(A) random selection, by each member  $i$ , of a number  $FK_{i,j}^{-1}$ ,

where  $0 \leq FK_{i,j}^{-1} \leq p-2$ , wherein  $p$  is a large odd prime number, such that  $p-1$  has large prime factors; and

(B) calculation, by each member  $i$ , of

$$5 \quad FK_{i,j} = \alpha_{i,j}^{FK_{i,j}^{-1}};$$

step (ii) comprises the step of calculation, by each member  $i$ , of  $HFK_{i,j} = (\alpha_{i,j} + FK_{i,j}) \bmod p$ ;

step (iii) comprises the step of encrypting, by each member  $i$ , of  $HFK_{i,j}$  in the form

$$10 \quad \left\{ \left\{ T_i, G, j, HFK_{i,j}, FK_{i,j} \right\}_{FK_{i,j-1}^{-1}} \right\}_{FK_{n,j-1}}$$

for transmission to each other member  $m$ ;

step iv) comprises the step of calculating, by each member  $i$ , of

$$\begin{aligned} \theta_{j+1} &= ((p-n-3) \theta_j + \sum_{i=1}^{i=n} HFK_{i,j}) \bmod (p-1) \\ &= GK_{j+1}^{-1}; \text{ and} \end{aligned}$$

15 step (v) comprises the step of calculation, by each member  $i$ , of

$$\alpha_{i,j+1} = (GK_{j+1}^{-1} + FK_{i,j}^{-1}) \bmod p.$$

9. The method of claim 1, wherein step c) comprises the steps of:

(i) sending, by a recovery initiator RI, of the hidden fractional key of a failed node  $\bar{i}$ ,  $HFK_{\bar{i},j}$ , to a newly elected member  $i$ , where  $j$  represents the iteration in which node  $\bar{i}$  failed;

20

(ii) sending, by RI, of  $SK_j$  to member  $i$ ;

WO 00/19652

PCT/US99/22710

-27-

(iii) performing a distributed initialization process, so that each member  $l$  receives a binding parameter  $\xi$  and a random pad  $\beta_{l,j}$ ;

(iv) calculation, by each member  $l$ , of  $HFK_{l,j} = \beta_{l,j} \diamond FK_{l,j}$ , where  $\diamond$  is a commutative operator;

5 (v) sending, by each member  $l$ , of  $HFK_{l,j}$  to member  $i$ ;

(vi) calculation, by member  $i$ , of

$$FK_{i,j} = \lambda \xi \diamond HFK_{1,j} \odot \dots \odot HFK_{n-1,j} \odot \theta_{j+1}, \text{ where } \odot \text{ is a}$$

commutative operator; and

(vii) calculation, by member  $i$ , of

10 
$$\alpha_{i,j} = HFK_{i,j} \odot FK_{i,j}$$

10. The method of claim 9, wherein

step (i) comprises the step of encrypting  $HFK_{i,j}$  in the form

$$\left\{ \left\{ T_{Ri}, R, j, HFK_{i,j} \right\}_{K_{Ri}^{-1}} \right\}_{Ki} \text{ for transmission to member } i, \text{ where } R \text{ indicates}$$

recovery mode;

15 step (ii) comprises the step of encrypting  $SK_j$  in the form

$$\left\{ \left\{ T_{Ri}, R, j, SK_j \right\}_{K_{Ri}^{-1}} \right\}_{Ki} \text{ for transmission to member } i; \text{ and}$$

step (v) comprises the step of encrypting  $HFK_{i,k}$  in the form

$$\left\{ \left\{ T_i, R, j, HFK_{i,j} \right\}_{K_i^{-1}} \right\}_{Ki}.$$

11. The method of claim 2, further comprising the step of

20 (d) verifying that each of initial pad  $\alpha_{i,j}$  has contributed to the calculation of  $\theta_1$ , performed after step (a).

WO 00/19652

PCT/US99/22710

-28-

12. The method of claim 11, wherein step (d) comprises the steps of:

(i) selection, by a predetermined member of the cluster, of a large prime  $q$ ;

(ii) distribution of  $q$  to all members;

5 (iii) selection, by the predetermined member, of a generator  $g$  of the multiplicative group under  $q$ ;

(iv) distribution of  $g$  to all members;

(v) selection by each member  $i$ , of a random polynomial  $f_i$  having a value of zero at the origin;

10 (vi) calculation, by each member  $i$ , of  $\hat{\alpha}_{i,j} = g^{\alpha_{i,j} + f_i}$ ;

(vii) sending, by each member  $i$ , of  $\hat{\alpha}_{i,1}$  to all other members;

(viii) calculation, by each member  $i$ , of

$$g^{\hat{\theta}_i} = \prod_{j=1}^{j=n} \hat{\alpha}_{i,j} = g^{\theta_i + \sum_{j=1}^{j=n} f_i}, \text{ evaluated at the origin};$$

(ix) determination, by each member  $i$ , of whether  $g^{\theta_i} = g^{\hat{\theta}_i}$ ,

15 evaluated at the origin; and

(x) determination, by each member  $i$ , of whether

$$g^{\alpha_{i,j}} = \frac{g^{\theta_i}}{\prod_{j=1}^{j=n} g^{\alpha_{j,1}}}.$$

13. The method of claim 4, further comprising the step of:

(e) verifying that each initial pad  $\alpha_{i,1}$  has contributed to the calculation of  $\theta_1$ , performed after step (a).

20

14. The method of claim 12, wherein step (e) comprises the steps of:

(i) selection, by a predetermined member of the cluster, of a large prime  $q$ ,

WO 00/19652

PCT/US99/22710

-29-

- (ii) distribution of  $q$  to all members;
- (iii) selection, by the predetermined member, of a generator  $g$  of the multiplicative group under  $q$ ;
- (iv) distribution of  $g$  to all members;
- 5 (v) calculation, by member 1, of  $g^y$  and  $g^{v_{1,1}}$ ;
- (vi) making  $g^y$  and  $g^{v_{1,1}}$  available to all members;
- (vii) calculation, by each member  $i$ , of  $g^{v_{i,1}}$ ;
- (viii) publication, by each member  $i$ , of  $g^{v_{i,1}}$  for other members of the cluster only;
- 10 (ix) determination, by each member  $i$ , of whether

$$g^{a_i} = \prod_{j=1}^{j=n} g^{v_{j,1}}.$$

15 15. A system for generating and managing shared keys for a plurality of members of a cluster, comprising

initialization means for performing system initialization to produce a fractionally generated initial shared key;

fractional generation means for fractional generation of a next shared key; and

recovery means for performing key recovery in the event of either compromise or failure of a node.

20 16. A computer program product comprising a computer usable medium having computer readable program code that executes on a computer that participates in the generation and management of shared keys for a plurality of members of a cluster, said computer readable program code comprising:

WO 00/19652

PCT/US99/22710

-30-

(a) first computer readable program code logic for causing the computer to participate in system initialization, wherein the initialization produces a fractionally generated initial shared key;

5 (b) second computer readable program code logic for causing the computer to participate in the fractional generation of a next shared key; and

(c) third computer readable program code logic for causing the computer to participate in key recovery in the event of either compromise or failure of a node.



WO 00/19652

PCT/US99/22710

1/11

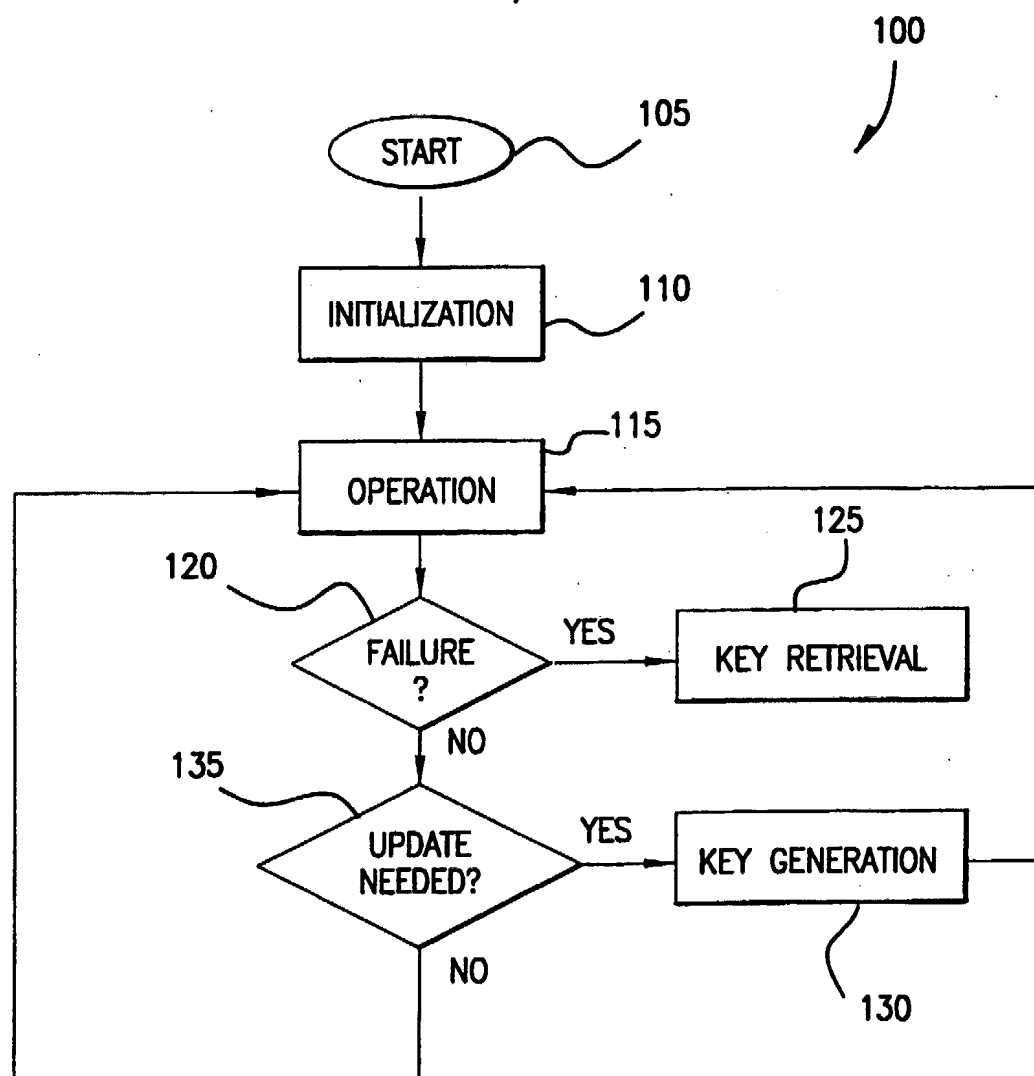


FIG.1

WO 00/19652

PCT/US99/22710

2/11

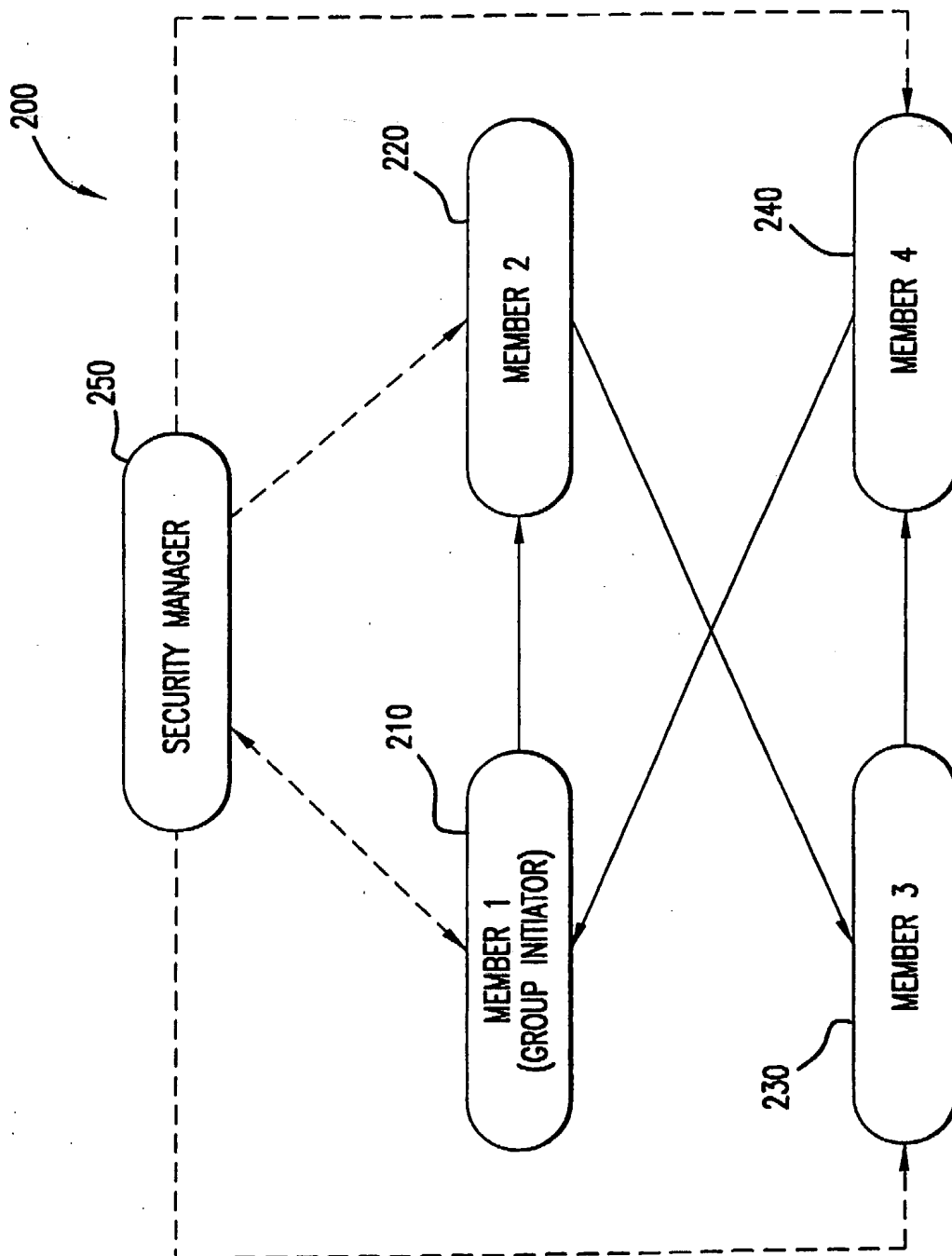


FIG. 2

WO 00/19652

PCT/US99/22710

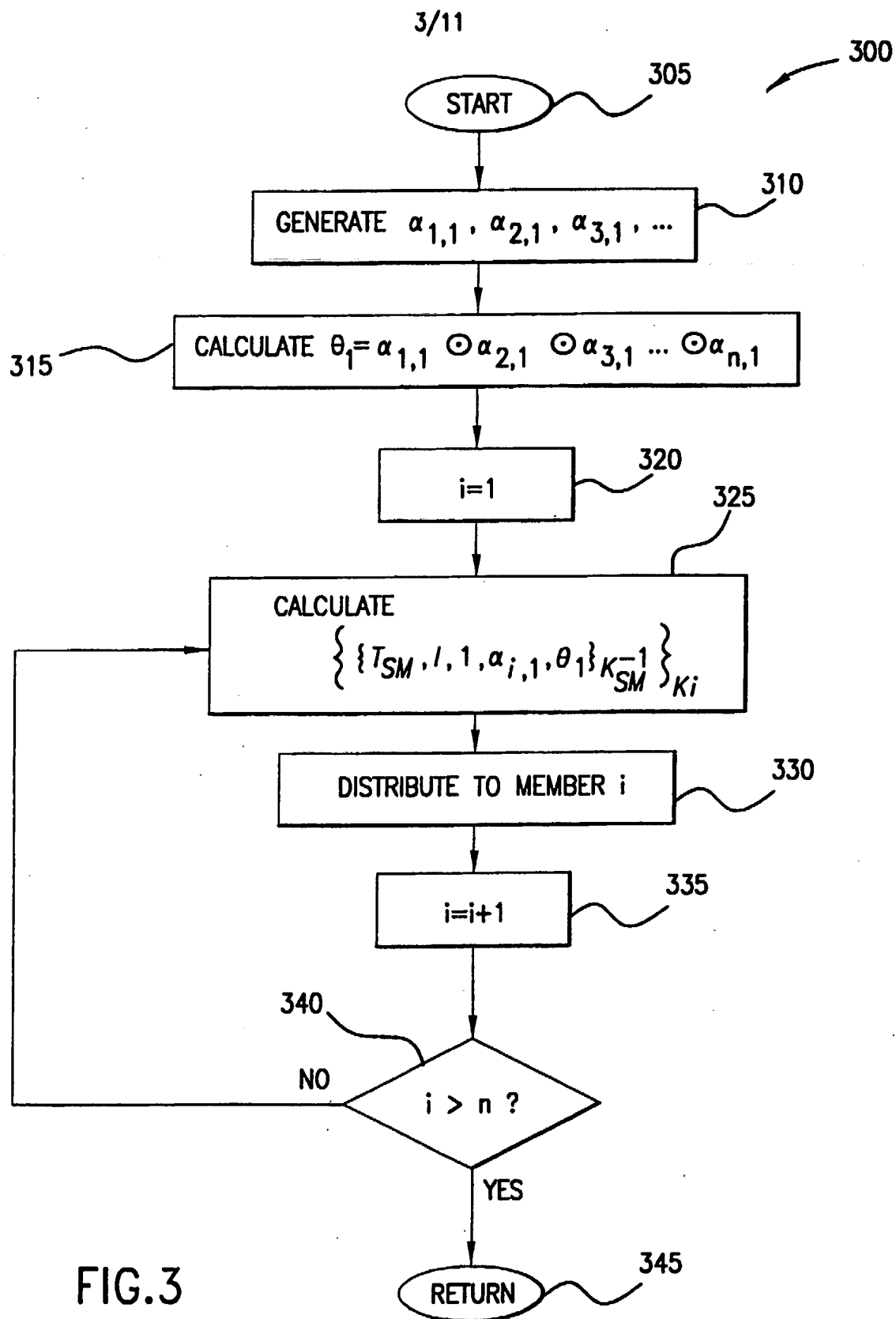


FIG.3

WO 00/19652

PCT/US99/22710

4/11

400

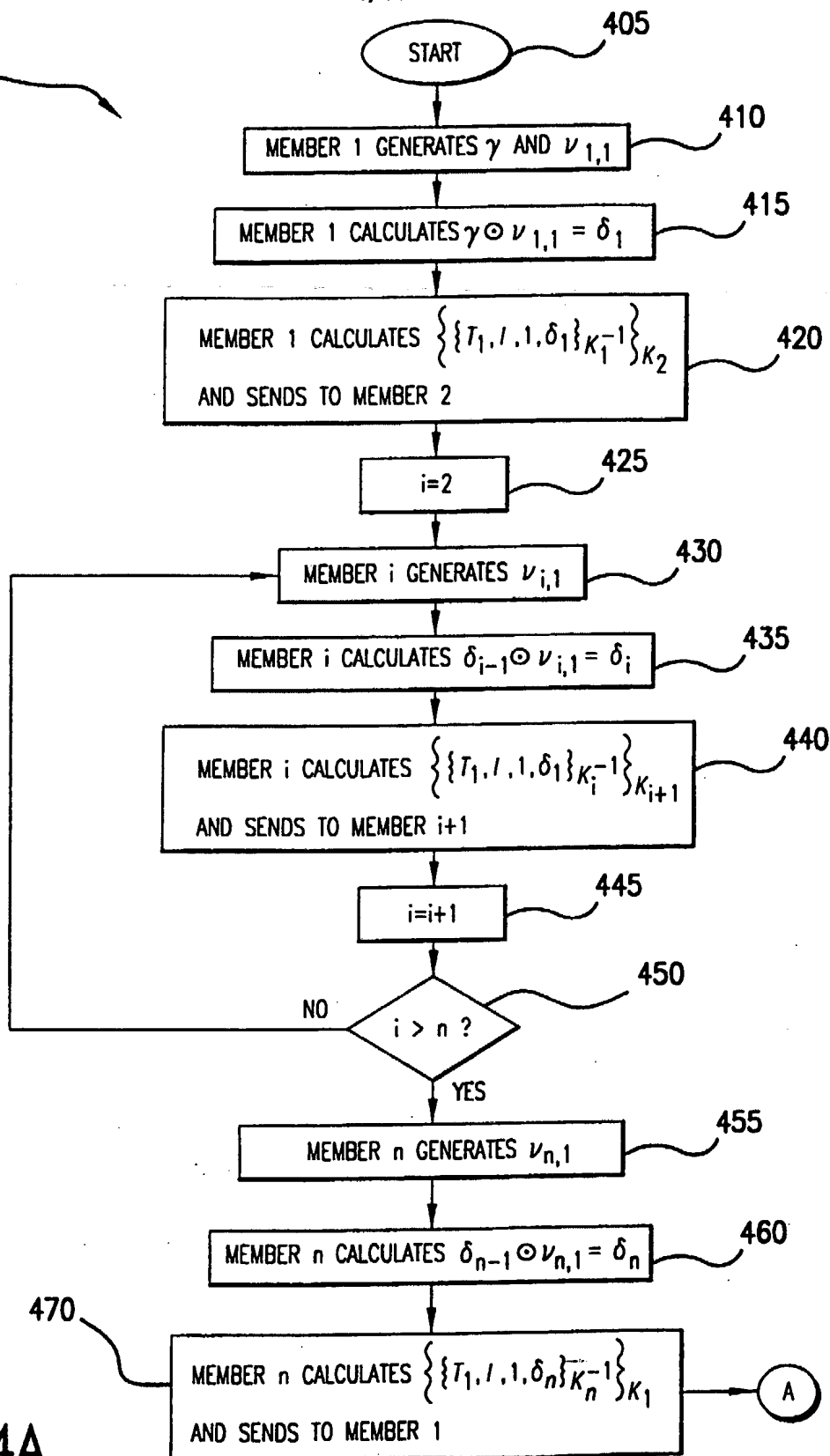


FIG.4A

WO 00/19652

PCT/US99/22710

5/11

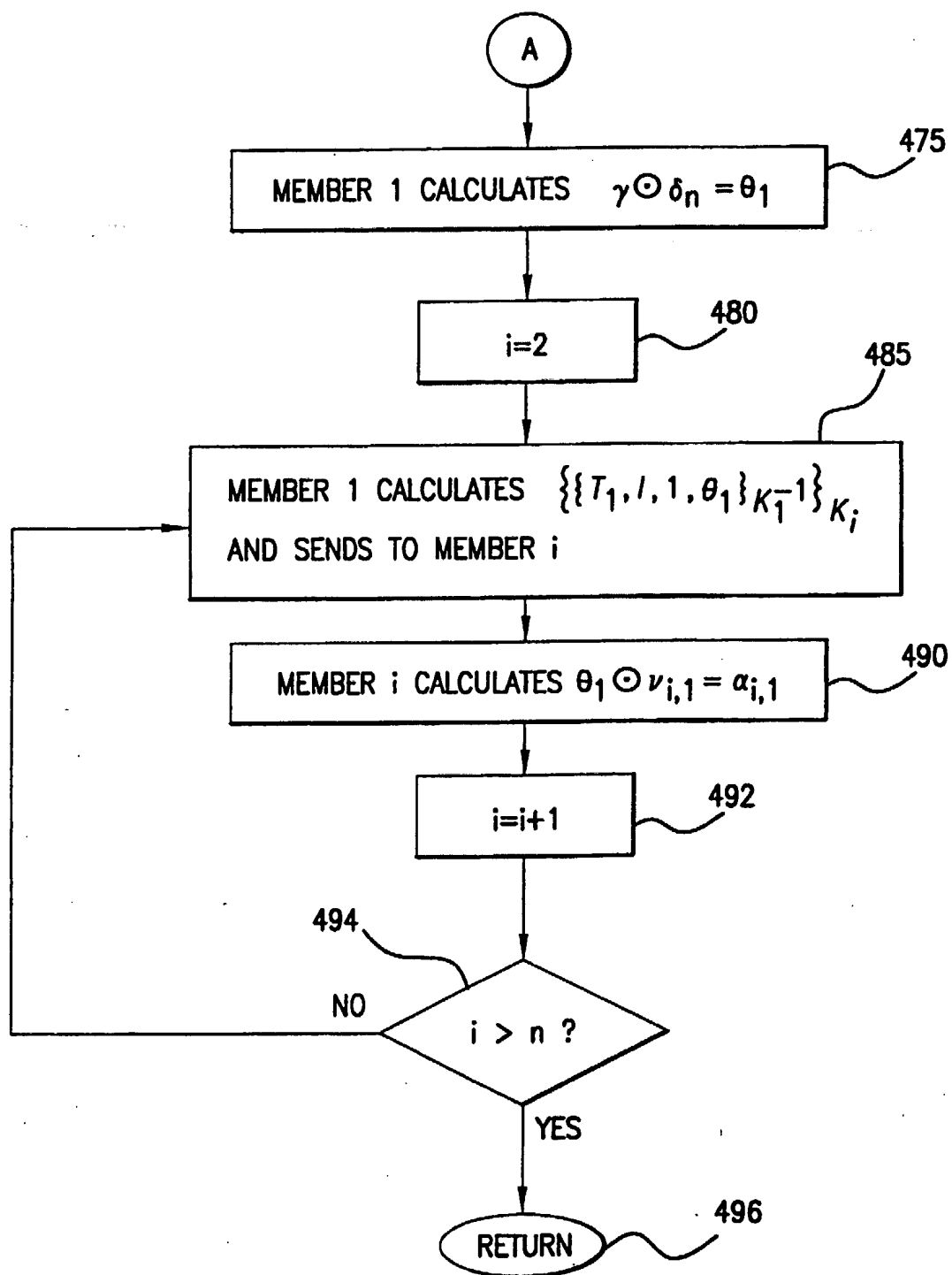


FIG.4B

WO 00/19652

PCT/US99/22710

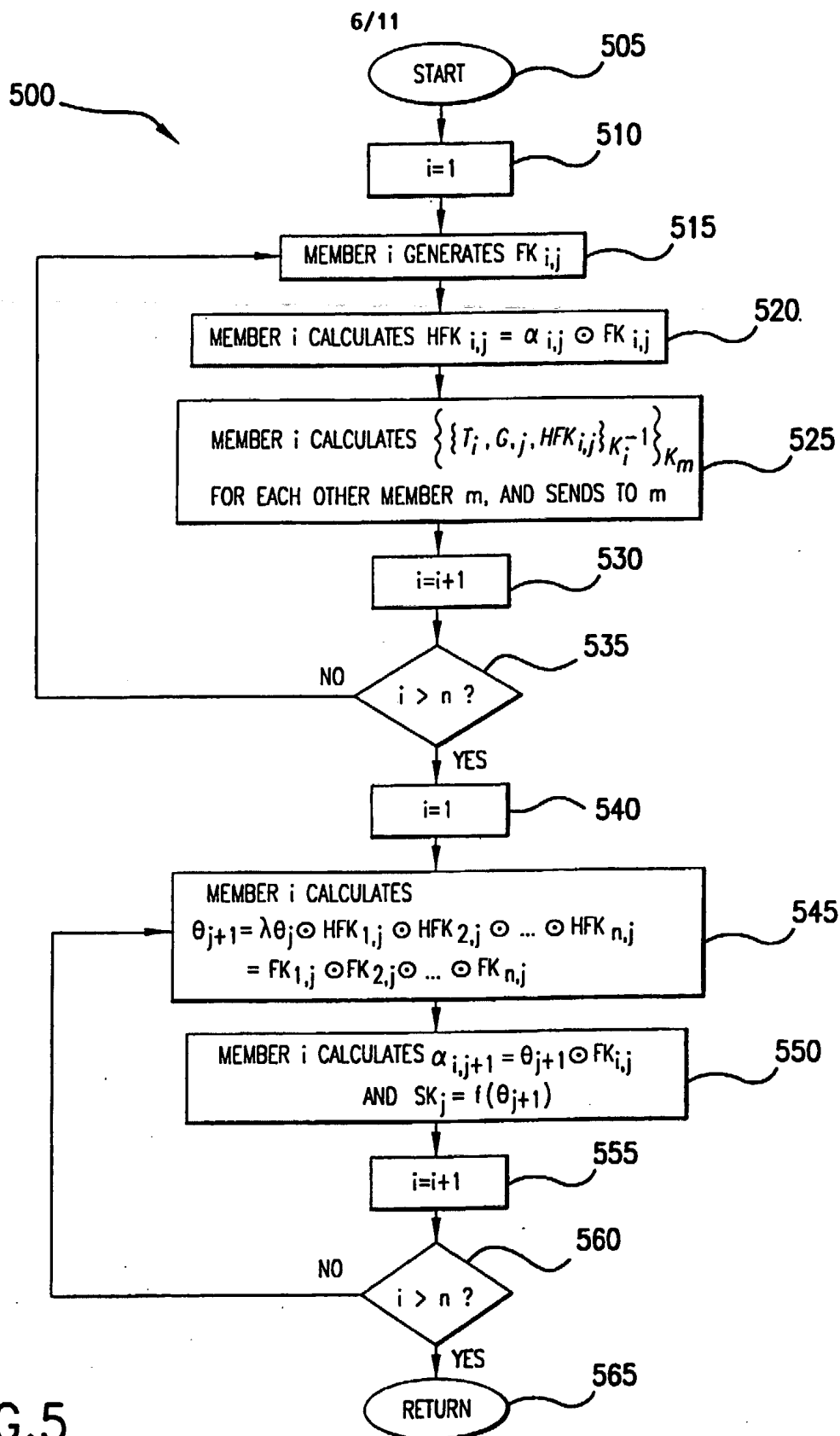


FIG.5

WO 00/19652

PCT/US99/22710

7/11

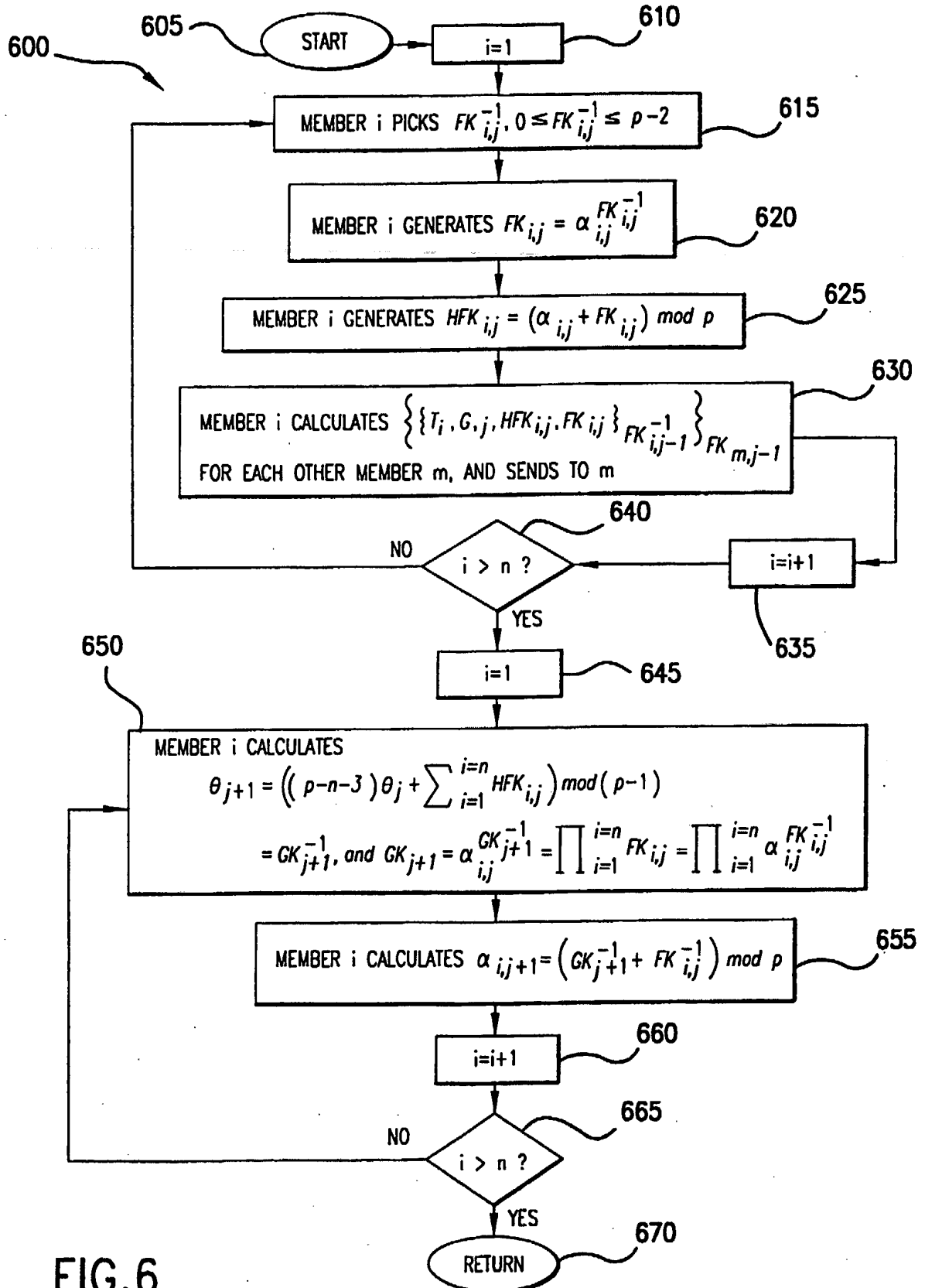


FIG. 6

WO 00/19652

PCT/US99/22710

8/11

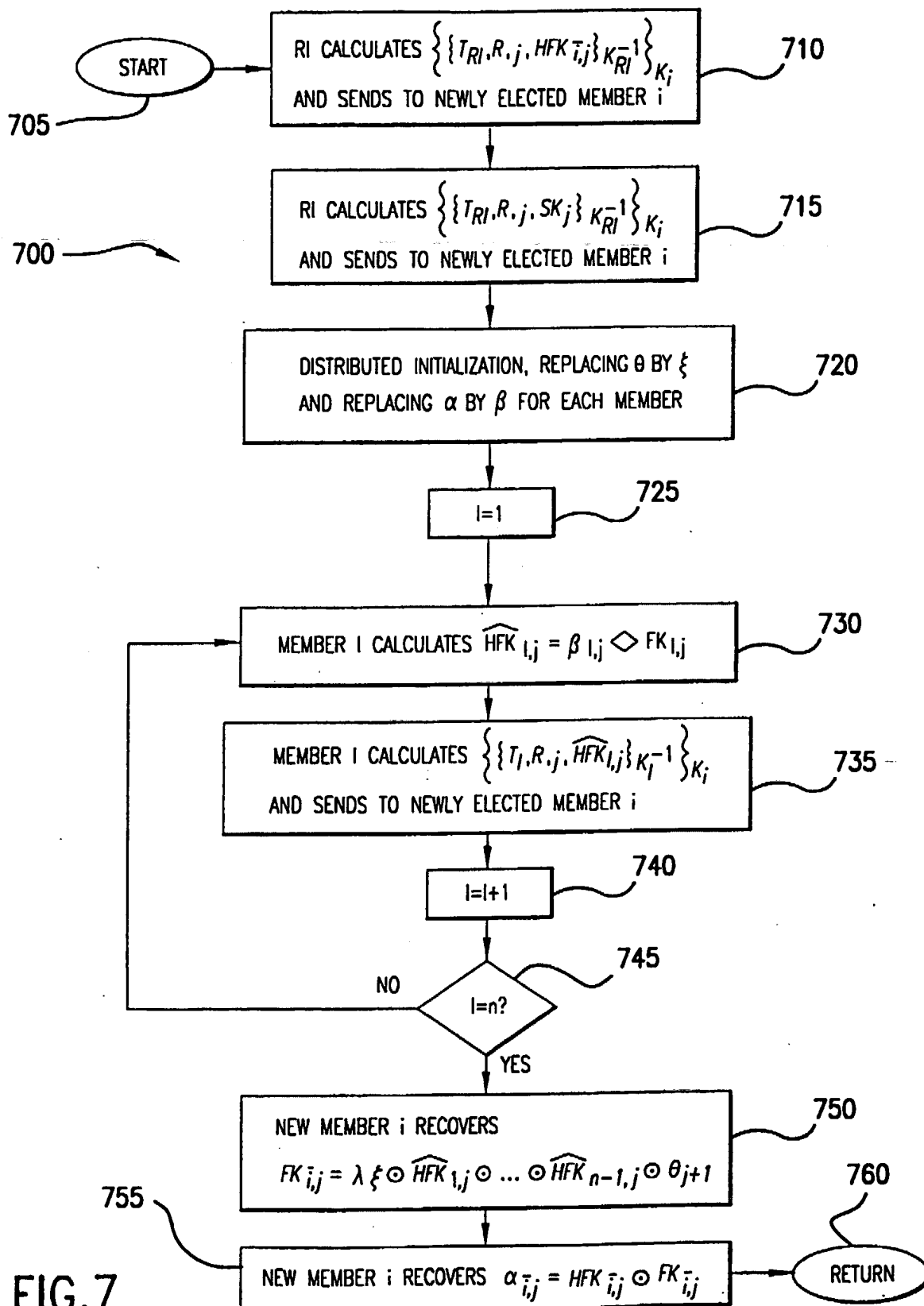


FIG. 7



WO 00/19652

PCT/US99/22710

9/11

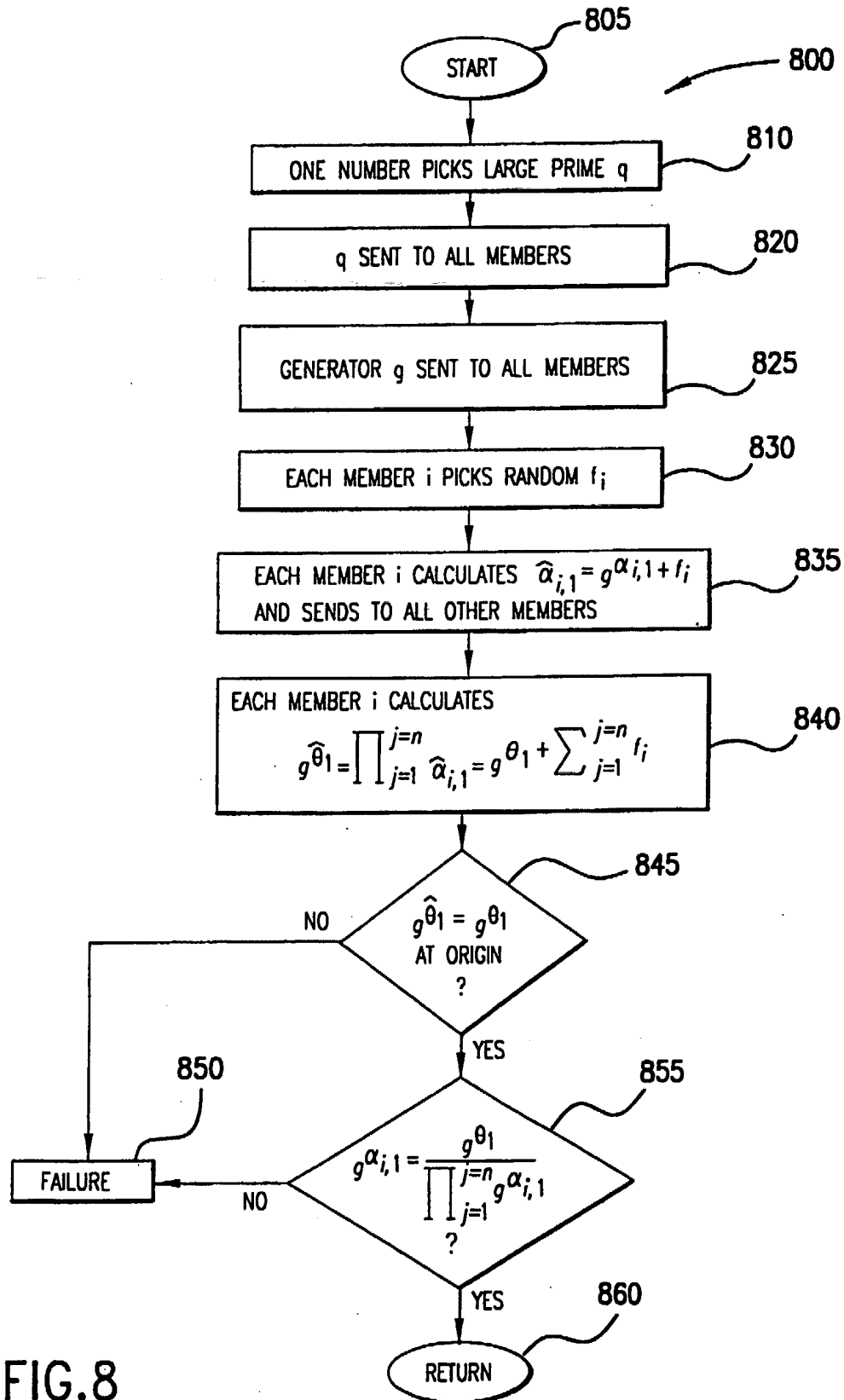


FIG.8

WO 00/19652

PCT/US99/22710

10/11

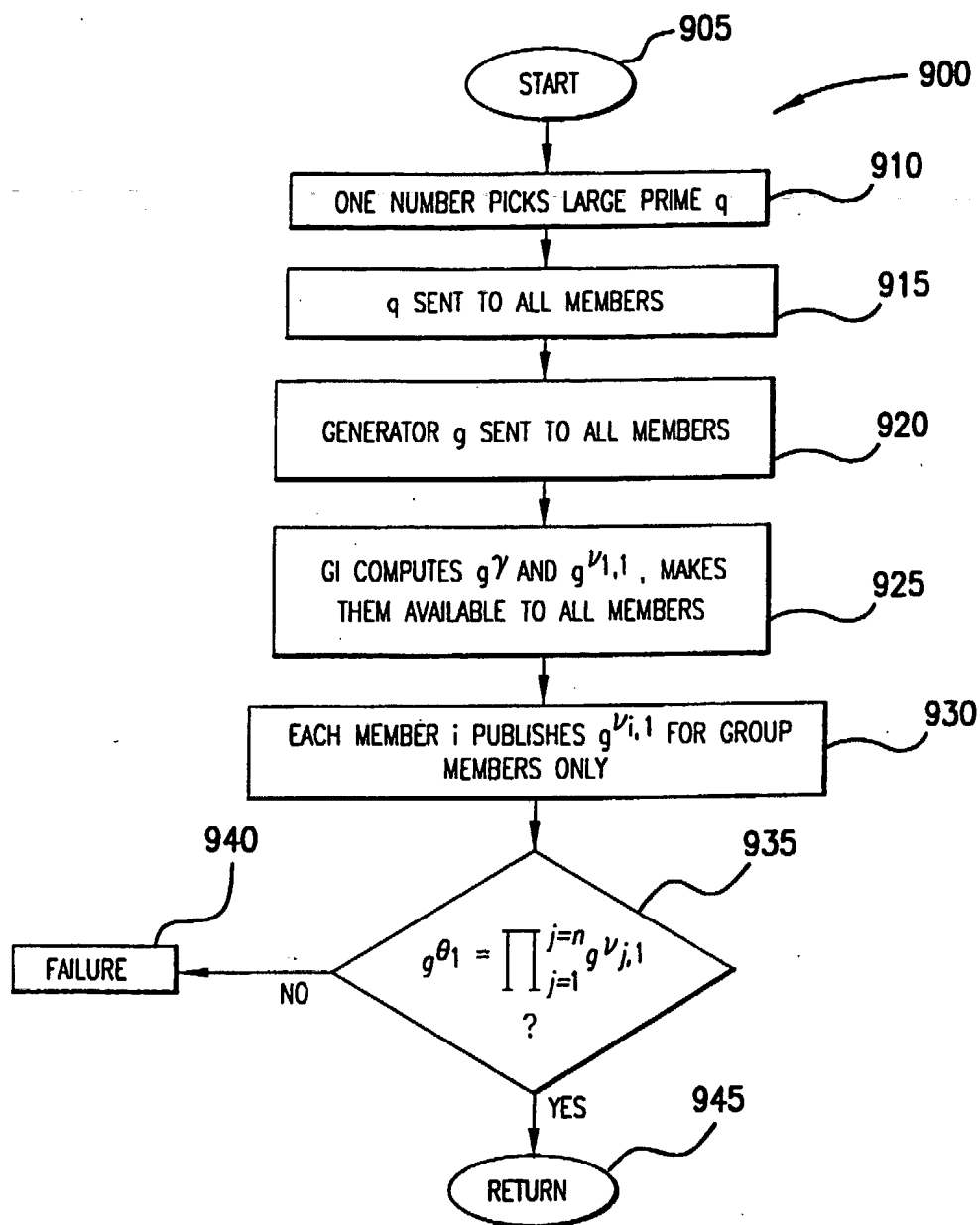


FIG.9

WO 00/19652

PCT/US99/22710

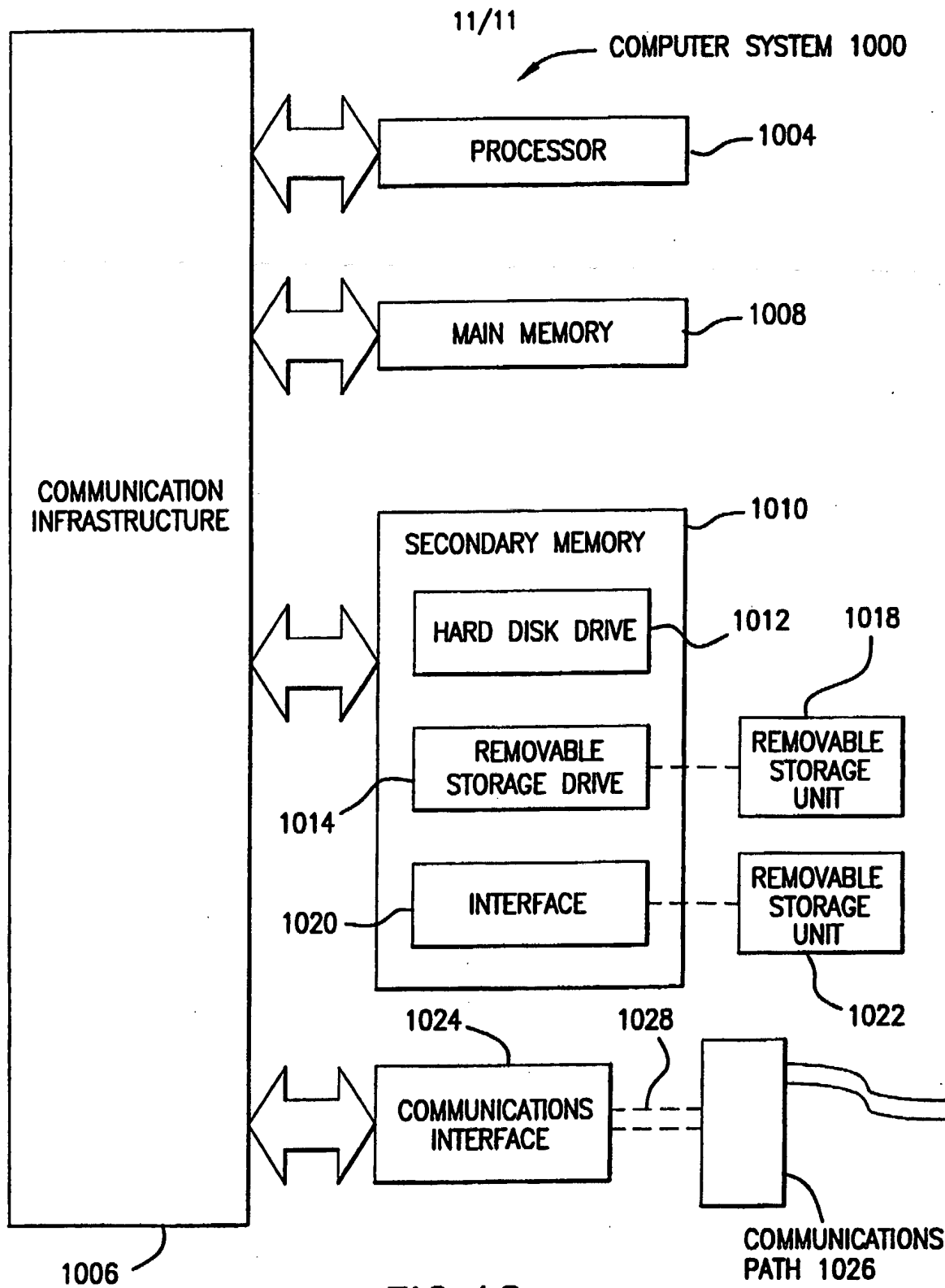


FIG.10

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US99/22710

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(6) : H04K 1/00

US CL : 380/283

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/259, 380/260, 380/262, 380/265, 380/277, 380/282, 380/283, 380/44, 380/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

STN/CAS WEST

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,625,692 A (HERZBERG et al.) 29 April 1997, col. 5 lines 2-7, col. 8, lines 10-20.	1
A, P	US 5,825,880 A (SUDIA et al.) 20 October 1998, entire document	1-16
A	US 5,708,714 A (LOPEZ et al.) 13 January 1998 entire document	1-16
A	US 5,675,649 A (BRENNAN et al.) 07 October 1997 entire document	1-16
A	US 5,276,737 A (MICALI) 04 January 1994 entire document	1-16

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
*A* document defining the general state of the art which is not considered to be of particular relevance	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
*B* earlier document published on or after the international filing date	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*Z* document member of the same patent family
*O* document referring to an oral disclosure, use, exhibition or other means	
*P* document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

22 DECEMBER 1999

Date of mailing of the international search report

16 FEB 2000

Name and mailing address of the ISA/US  
Commissioner of Patents and Trademarks  
Box PCT  
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

PAUL E. CALLAHAN

Telephone No. (703) 305-1336